Carnegie Mellon
Software Engineering Institute
Pittsburgh, PA 15213-3890

Applying Critical Success Factors to Information Security Planning

Richard A Caralli, William R Wilson
Survivable Enterprise Management Team

Networked Systems Survivability
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Sponsored by the U.S. Department of Defense

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JAN 2004		**00-00-2004 to 00-00-2004**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Applying Critical Success Factors to Information Security Planning	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University,Software Engineering Institute,Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**42**	

Carnegie Mellon
Software Engineering Institute

Objectives

Introduce the concept of critical success factors

Illustrate the use of critical success factors as a foundation for security management

Provide real world examples in developing and analyzing critical success factors

Carnegie Mellon
Software Engineering Institute

Agenda

Introduction

CSF Concepts

Applying CSFs to security

Summary

Field observation

Enterprise security strategies are ineffective in the long run when they do not focus on and align with organizational drivers

Carnegie Mellon
Software Engineering Institute

How do we fix it?

Base organizational strategy and security strategy on the **same** organizational drivers

- Mission is good, but abstract and open to interpretation
- Goals are better, but more operational in nature
- **CSFs are more reliable and universal**—key performance factors that all levels of management must consider

Carnegie Mellon
Software Engineering Institute

Introduction to Critical Success Factors

Carnegie Mellon
Software Engineering Institute

CSFs defined

The limited number of areas in which satisfactory results will ensure competitive performance for the organization and enable it to achieve its mission

Key areas of activities

- in which favorable results are necessary to achieve goals.
- where things must go right for the organization to flourish.
- that should receive constant attention from management.

CSF examples

Automobile industry

"Meet federal energy standards for automobiles."

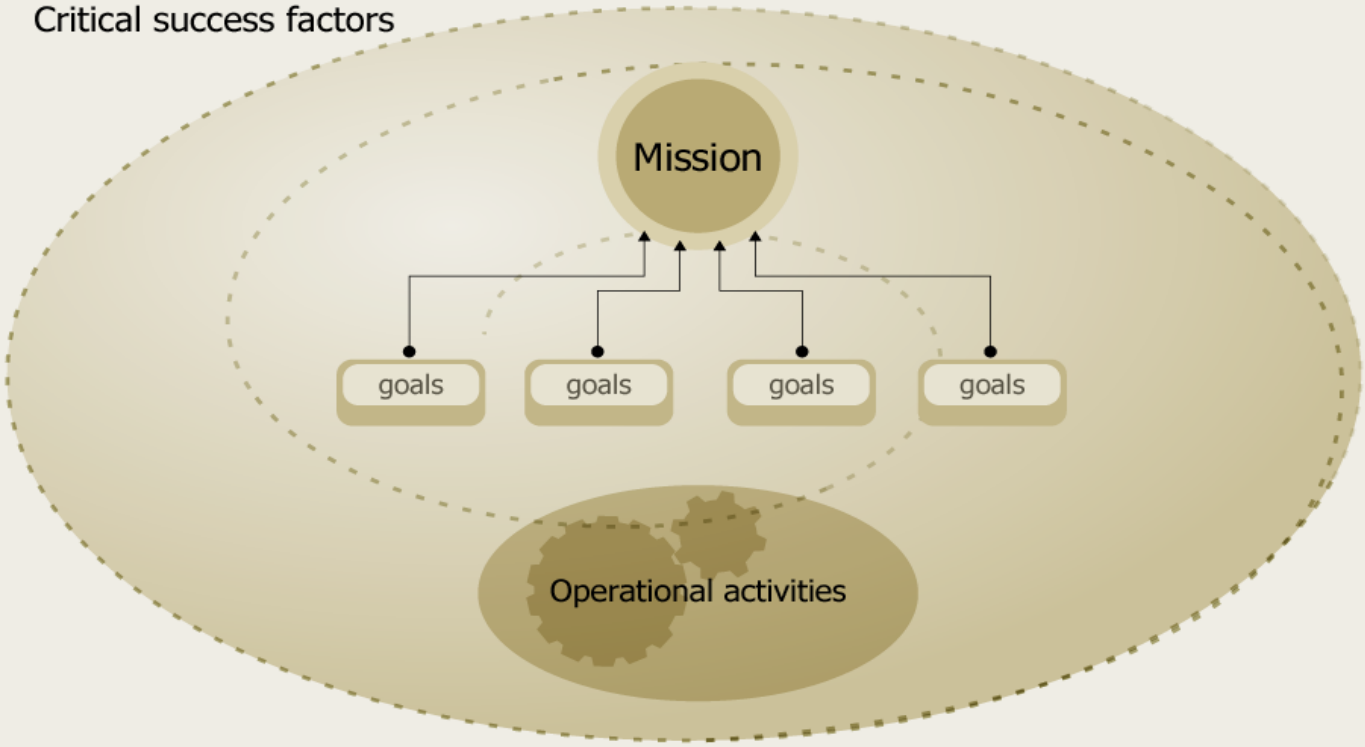
County government

"Deliver high-quality, low-cost citizen services."

Educational institution

"Attract and retain high-quality faculty."

CSFs are the glue



Characteristics of CSFs

Sources define the various entities where CSFs originate

Dimensions describe the properties of CSFs relative to perspective (internal vs. external) and function (monitoring vs. adapting)

Hierarchy describes the relationship between CSFs at the various layers of an organization

Five sources of CSFs

Industry in which the organization operates

Organization's relationship with its **peers**

Environmental factors that the organization can't control

Temporary barriers, challenges or problems

Domain of each layer of management

Sources of CSFs

Internal vs. External CSFs

Internal CSFs are within the span of control for a particular manager

External CSFs are most likely not controllable by a particular manager

An awareness helps managers actively set better goals and predict potential impacts when CSFs are not achieved

Monitoring vs. Adapting CSFs

Monitoring CSFs emphasize the continued scrutiny of existing situations

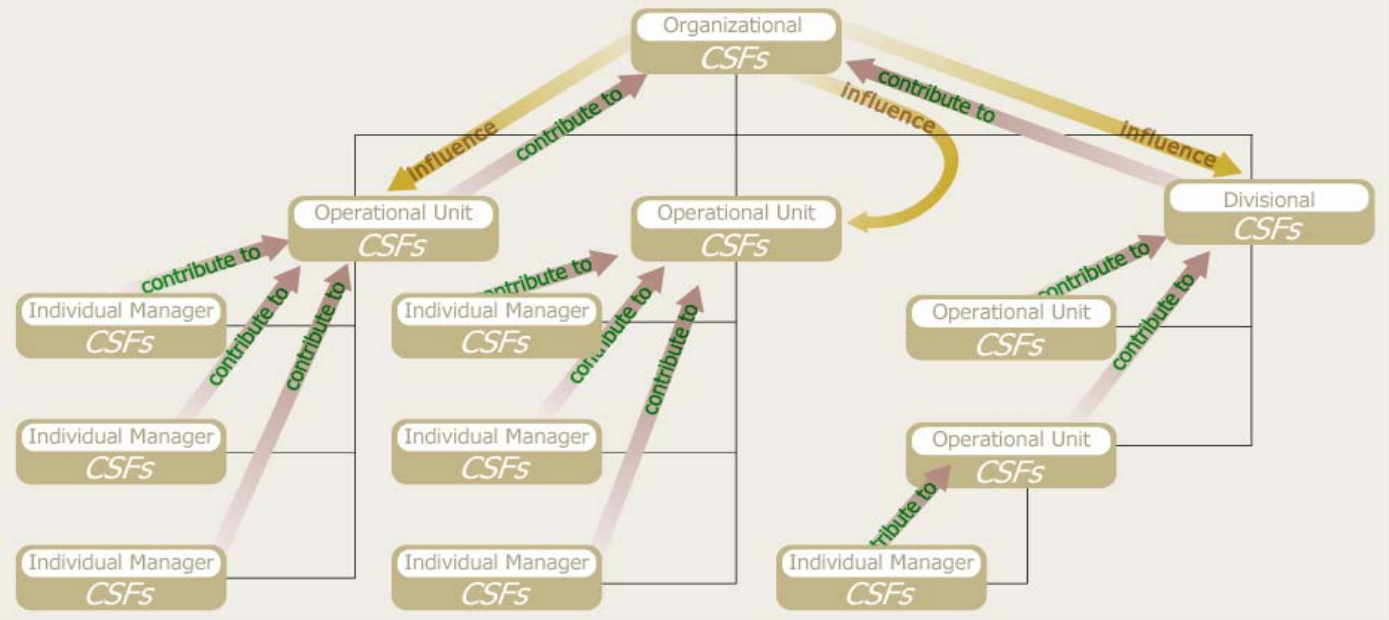
Adapting CSFs focus on improving and growing the organization

Managers almost always have monitoring CSFs

Adapting CSFs most likely to be confused with goals

Hierarchy of CSFs

CSFs exist throughout the organization at every management layer and level



The CSF Method

Carnegie Mellon
Software Engineering Institute

Five key activities

Defining scope

Collecting data

Analyzing data

Deriving CSFs

Analyzing CSFs

Organizational CSF participants

Specific *roles*:

- C-level executives
- Vice-President and director level
- Division heads
- Chief Legal Counsel
- Corporate Secretary
- VP Investor Relations, M & A, Marketing & Sales, PR
- Strategic Planners

Unique *functions*:

- Asset management
- Corporate reporting and taxes
- Risk Management
- Controller and treasurer
- Government relations
- Select Board members
- Select external personnel

Interview questions -1

What are the CSFs in your job right now?

In what 1, 2, or 3 areas would failure hurt you most?

In what area would you hate to see something go wrong?

Assume you are placed in a dark room with no access to the outside world. What would you most want to know about the organization when you emerged three months later?

Carnegie Mellon
Software Engineering Institute

Interview questions -2

What is your personal mission and role in the organization?

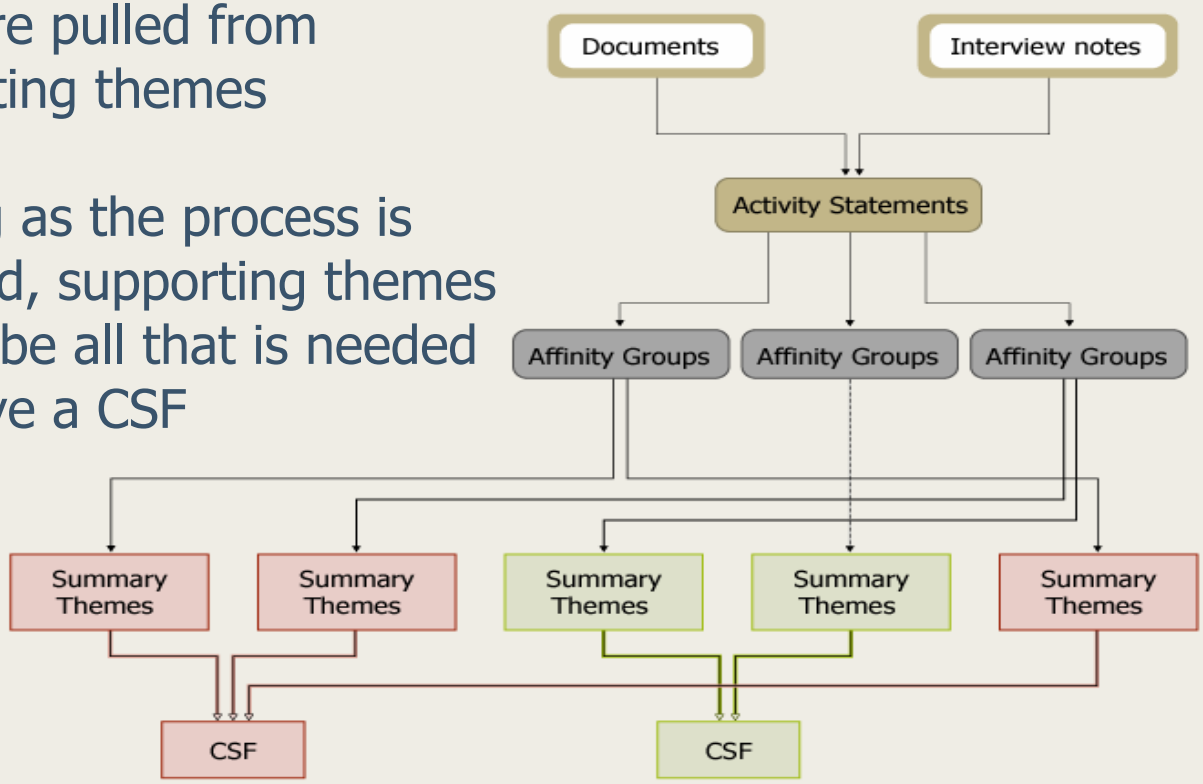
What are your most critical goals and objectives?

What are your three greatest business problems or obstacles?

Deriving CSFs

CSFs are pulled from supporting themes

So long as the process is followed, supporting themes should be all that is needed to derive a CSF



Carnegie Mellon
Software Engineering Institute

CSF approach advantages

Guarantee alignment with organizational drivers

Reduce organizational ambiguity

Dependable guiding force/target for the organization

Reflect current operating environment of the organization

Reflect management's risk perspective

Course correction

Carnegie Mellon
Software Engineering Institute

Applying CSFs to Enterprise Security Management

Carnegie Mellon
Software Engineering Institute

Areas of promise using CSFs

As a tool for information security risk management

Providing impetus for managing security as a process throughout the organization

Foundation for enterprise resiliency

Carnegie Mellon
Software Engineering Institute

CSFs can enhance ISRM

Determining risk assessment scope

Selecting critical assets for assessment

Identifying and validating security requirements

Identifying risks to critical assets

Setting evaluation criteria for measuring risk

Evaluating threats and mitigating risk

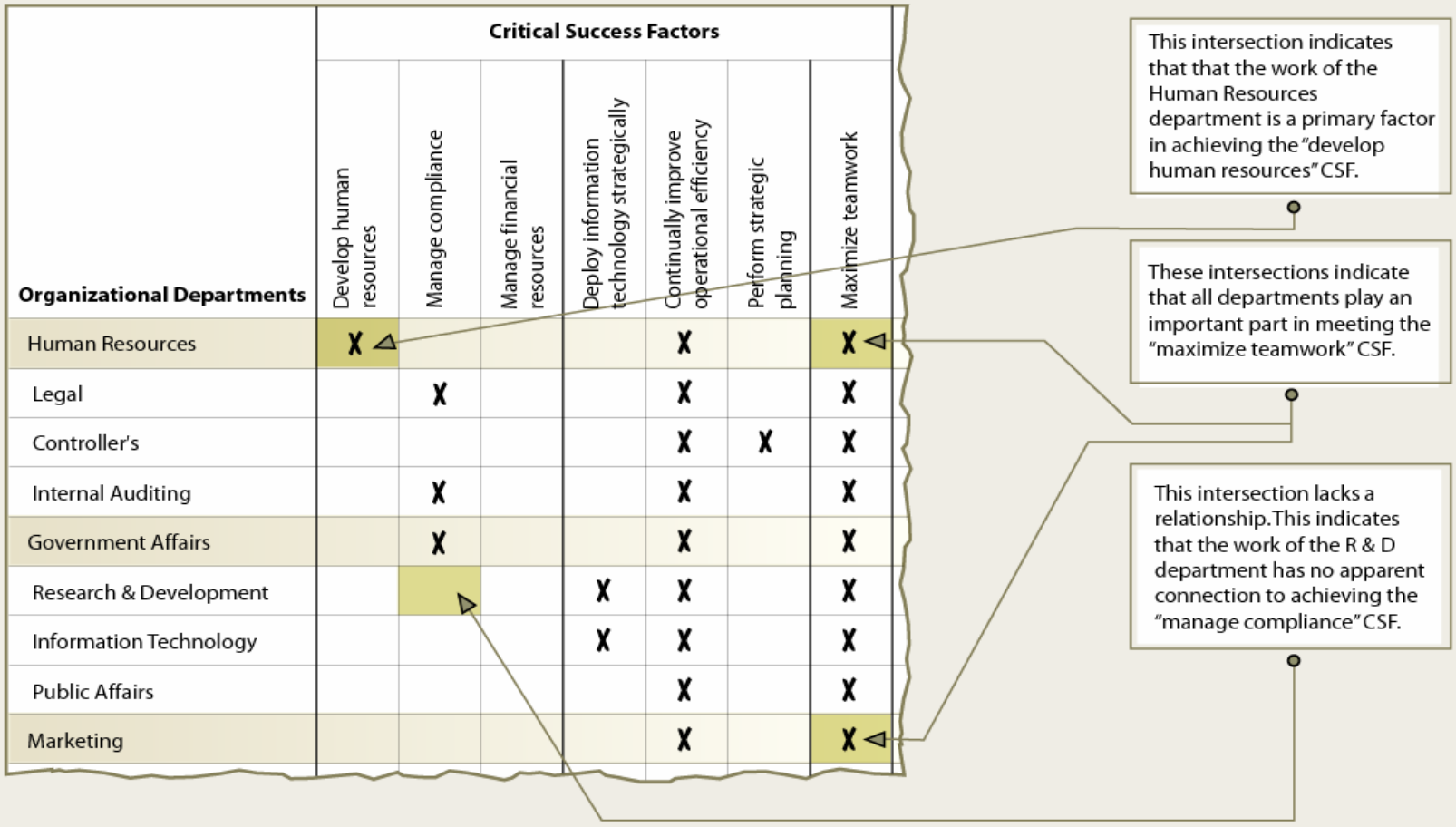
Using CSFs to set scope

Most important and difficult task in risk assessment

Failure to focus a risk assessment on the right areas of the organization will not yield meaningful results

Using affinity analysis, focus on those areas that are most important to accomplishing the organization's mission

Scope example



Carnegie Mellon
Software Engineering Institute

CSFs and critical assets

Risk-based approach to information security directs resources to protecting the organization's most **critical assets**

Selection of assets to protect is often left to judgment or perceived value

CSFs can aid in identifying an organization's critical assets—those that contribute most to accomplishing the organization's mission

Critical assets example

Critical Assets	Critical Success Factors						
	Develop human resources	Manage compliance	Manage financial resources	Deploy information technology strategically	Continually improve operational efficiency	Perform strategic planning	Maximize teamwork
Customer information					X		
Payroll information			X				
ERP system					X		
Financial data		X	X				
Widget formulas					X		
EIS system						X	
Skills database	X						X

The asset "financial data" is important for managing compliance.

Carnegie Mellon
Software Engineering Institute

CSFs and security requirements

An important component of protecting critical assets

Foundation for devising an appropriate protection strategy for the assets

Prioritization of the requirements is necessary to determine which requirement, if unmet, would impact the owner of the asset and the organization

CSFs can aid in this prioritization of requirements.

Security requirements example

Critical Assets and Security Requirements	Critical Success Factors						
	Develop human resources	Manage compliance	Manage financial resources	Deploy information technology strategically	Continually improve operational efficiency	Perform strategic planning	Maximize teamwork
Medical records							
confidentiality		X					
integrity							
availability					X		
Widget formulas							
confidentiality							
integrity							

A violation of the confidentiality requirement impedes the ability to manage compliance.

CSFs and risk identification -1

At the core of a risk management approach to security

Two popular means:

- Use a taxonomy as a guide
- Rely upon organizational judgment

Both methods can overlook common risks or risks unique to an organization

CSFs can sharpen focus on important risks

Carnegie Mellon
Software Engineering Institute

CSFs and risk identification -2

Properly focus risk identification in the right areas

Shape and guide the knowledge or input from personnel in the organization

Validate and prioritize risks that have been identified

CSFs and measuring risk

Requires evaluation criteria

Organization-based criteria likely to reflect unique drivers, but not guaranteed

Criteria can be validated (to ensure alignment with organizational drivers) by comparison to the organization's CSFs

Evaluation criteria example

Evaluation criteria	Critical Success Factors						
	Develop human resources	Manage compliance	Manage financial resources	Deploy information technology strategically	Continually improve operational efficiency	Perform strategic planning	Maximize teamwork
Reputation			X		X	X	
Life & health		X	X				
Fines & legal penalties			X				
Financial			X				
Productivity	X				X		X

The "productivity" criterion is an area of risk impact measurement that relates to the "develop human resources" CSF.

Carnegie Mellon
Software Engineering Institute

CSFs and risk mitigation

Depends on prioritization of those risks that most impact the organization

The organization is impacted whenever its ability to conduct its normal course of business is impeded.

Comparing risks to CSFs identifies those risks that are candidates for mitigation because

- they interfere with the achievement of CSFs and
- they affect other organizational drivers (goals, etc.)

Risk mitigation example

Risks to Critical Assets	Critical Success Factors						
	Develop human resources	Manage compliance	Manage financial resources	Deploy information technology strategically	Continually improve operational efficiency	Perform strategic planning	Maximize teamwork
Widget formulas							
Stolen and sold					X		
Altered					X		
Destroyed by flood					X		
Employee records							
Altered		X					
Customer information							
Destroyed		X	X			X	

This risk should be considered for mitigation because it potentially impedes the "manage compliance" CSF.

Enterprise resiliency -1

Physical property of a material that allows it to spring back after deformation that has not exceeded its elastic limit [www.cogsci.princeton.edu]

". . .ability to withstand systemic discontinuities" [Booz Allen]

". . .ability to adapt to new risk environments" [Booz Allen]

Source: Booz Allen - Enterprise Resilience: Managing Risk in the Networked Economy

Enterprise resiliency -2

Carnegie Mellon
Software Engineering Institute

Summary and conclusions

CSFs relate to the core functions of management—planning, organizing, coordinating, directing, and controlling

CSFs are essentially a management tool for better decision making that aligns with the organization's business drivers

CSFs show significant promise as a tool for improving enterprise security management by helping to ensure that security strategy actually enables the achievement of the organizational mission

Carnegie Mellon
Software Engineering Institute

For more information

Networked Systems Survivability Program
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213 USA

http://www.cert.org
http://www.sei.cmu.edu

William Wilson
wrw@sei.cmu.edu

Carnegie Mellon
Software Engineering Institute

Presentation references

John F. Rockhart, "Chief Executives Define Their Own Data Needs," Harvard Business Review, (1979)

John F. Rockhart & Bullen, Christine V, "A Primer on Critical Success Factors," CISR Working Paper No. 69, June 1981. © 1981 Massachusetts Institute of Technology. Used with permission.

Randy Staff, Jim Newfrock, and Michael Delurey, "Enterprise Resilience: Managing Risk in the Networked Economy," Enterprise Resilience: Risk and Security in the Networked World, 2003 Booz Allen Hamilton; www.strategy-business.com